

February 6, 2001

INSPECTOR GENERAL INSTRUCTION 7950.4

SUBJECT: Microcomputer Antivirus Program

References. See Appendix A.

A. Purpose. This Instruction updates the Office of the Inspector General, Department of Defense (OIG, DoD), Microcomputer Antivirus Program. Additionally, it provides procedures for dealing with suspected virus attacks.

B. Cancellation. This Instruction supersedes IGDINST 7950.4, *Microcomputer Antivirus Program*, August 18, 2000.

C. Applicability

1. This Instruction applies to the Office of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; Director, Intelligence Review; and the Office of the Deputy General Counsel (Inspector General), which is provided support by the OIG, DoD. These organizations are referred to collectively as OIG components.

2. This Instruction applies to all microcomputers belonging to the OIG, DoD, anywhere in the world, whether or not they are connected to the OIG Local Area Network (LAN) or the OIG Wide Area Network (WAN).

D. Definitions. See Appendix B.

E. Introduction of Malicious Software

1. End users, either intentionally or unintentionally, can introduce malicious software into the OIG, DoD, environment. This software (often referred to as a computer "virus") can replicate itself, propagate through microcomputers by itself, and cause vast amounts of damage. Microcomputers generally have more limited technical controls and less management oversight than any other type of computer. Therefore, they are more dependent on end users for the effective implementation of protective measures.

2. Contact with viruses occurs when end users introduce new hardware or software into the OIG, DoD, environment. Frequent sources of viruses include:

- a. Microcomputers, floppy disks, Zip disks, or CD media previously used outside the OIG, DoD, environment.
- b. Illegal use of bootleg software.
- c. Software downloaded from electronic bulletin board systems.
- d. Electronic mail messages, attachments to electronic mail messages, or software downloaded from the Intranet or Internet.

Report Documentation Page

Report Date 06 Feb 2001	Report Type N/A	Dates Covered (from... to) - -
Title and Subtitle Microcomputer Antivirus Program		Contract Number
		Grant Number
		Program Element Number
Author(s)		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884		Performing Organization Report Number
Sponsoring/Monitoring Agency Name(s) and Address(es)		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified		Classification of this page unclassified
Classification of Abstract unclassified		Limitation of Abstract UU
Number of Pages 8		

IGDINST 7950.4

e. Commercially obtained hardware or software tampered with in the manufacturing or distribution process.

F. Policy

1. The OIG, DoD, shall concentrate on minimizing opportunities for introduction of viruses through end user protective measures and compliance with DoD and OIG policies.

2. Failure to adhere to this Instruction could result in discontinuance of end user access to the OIG, DoD, LAN/WAN and/or disciplinary action. Employees who negligently or intentionally misuse microcomputers may be subject to criminal prosecution, civil fines and penalties, and/or agency administrative actions. Administrative actions could include disciplinary action up to and including removal from the Federal service and/or revocation of a security clearance and/or continued employment in a sensitive position. The type of action taken depends on the violation. When such actions are taken, applicable laws, regulations, and procedures are followed, including, but not limited to, reference a.

3. End users shall immediately report any violation of this Instruction to their immediate supervisor, the OIG Security Division, Personnel and Security Directorate (PSD), and the Information Systems Directorate (ISD), Office of Administration and Information Management (OA&IM).

G. Responsibilities

1. The **ISD, OA&IM**, shall:

a. Develop instructions for antivirus software use.

b. Coordinate the OIG Microcomputer Antivirus Program.

c. Designate an antivirus administrator and a back up antivirus administrator. The antivirus administrator shall install antivirus software on OIG, DoD, servers, update antivirus software on a routine basis, administer installation of antivirus software on end user computers, monitor antivirus software use, support the repair or removal of infected files discovered on OIG, DoD, computer hardware and software, and perform other antivirus administrative functions.

d. Provide antivirus software updates with installation instructions to all end users at reasonable time intervals.

e. Create and maintain a library of up-to-date virus scanning and eradication software.

f. Return the end user to the standard OIG, DoD, configuration when the ISD determines that hardware or software introduced by the user are causing malfunctions of standard OIG, DoD, hardware or software in accordance with reference b. While every effort shall be made to recover critical data, the ISD shall not assume responsibility for any lack of functionality or any loss of data by return to the standard OIG, DoD, configuration.

g. Determine whether to restore network access, in consultation with the Employee Relations Division (ERD), PSD, to end-users whose password and/or user identification are disabled.

h. Scan commercially purchased software with virus eradication software before use on an OIG, DoD, microcomputer. When software is purchased in quantity, scan one copy per batch before the software is distributed and loaded on OIG, DoD, microcomputers. Scanning shall be documented before distribution.

i. Provide written notification to the head of the affected component; the OIG Security Division; ERD, PSD, and the Chief Information Officer (CIO) of a virus attack, stating the nature of the virus, effects on hardware or software, damage, possible origin, and corrective action taken to repair any damage.

j. Refer apparent violations of this policy for further investigation to appropriate parties.

2. **End Users** shall:

a. Operate the hardware or software within established laws, guidelines, and procedures, including software licensing agreements.

b. Minimize the use of bootable floppy diskettes or other bootable media on ISD-provided computers.

c. Scan hardware or software used outside the OIG, DoD, environment before reintroducing it to the OIG, DoD, environment.

d. Be alert to symptoms that can occur when a computer virus infects a microcomputer, such as continuous rebooting, an unexpected message or an electronic mail message with suspicious information.

e. Lock the computer by using a software lock, logout of the OIG, DoD, LAN/WAN, or reboot microcomputers when leaving the microcomputer unattended or upon completion of the work performed. If users are connected to a system maintained outside the OIG, DoD, they shall follow supplied log off instructions.

f. Write-protect floppy diskettes unless copying or saving data to the diskette.

g. Protect user identifications and passwords from compromise.

h. Regularly scan hard disks, floppy diskettes, Zip disks, and CD media for viruses.

End users should ask their Information Systems Liaison Working Group (ISLWG) representatives or the Information Center (IC) for assistance if they are unfamiliar with the process of scanning.

i. Ensure current antivirus software and current virus definition files are installed on each microcomputer on a weekly basis. End users should ask their ISLWG representatives or the IC for assistance if they are unfamiliar with the update process.

j. Regularly back up data by copying data to media other than where the data is currently stored.

k. Not disable antivirus software settings and not remove antivirus software from any microcomputer unless ISD instructs the software be removed.

l. Report suspected virus attacks to the ISD in accordance with reference c and component-established procedures.

3. **The OIG Component Heads** shall:

a. Devise internal procedures to ensure implementation of the provisions of this Instruction and references b through g, including internal management control mechanisms.

- b. Prepare necessary justifications for restoration of end user access.
- c. Contact the ERD for advice and assistance in determining appropriate disciplinary or administrative action. Coordinate disciplinary action, if any, with the ERD.

4. The **PSD, OA&IM**, shall:

- a. Assist and advise the OIG Component Heads on appropriate disciplinary actions if an end user violates this Instruction.
- b. Conduct a security review, when appropriate.

5. The **Component Information System Security Officer (ISSO)** shall oversee the provisions set forth in this Instruction.

H. Procedures

1. End users shall ensure that their microcomputers are scanned at least once each working day. If the automated scan set by ISD is not running as scheduled, the end user shall perform this scan manually and notify the IC that the automated scan is not working. The OIG Component Heads may encourage automatic virus scanning during non-duty hours for more efficient use of microcomputers during the duty day.

2. End users shall ensure that every floppy disk, Zip disk, CD media, or any information downloaded from an external source is scanned. Floppy disks, Zip disks, and CD media cases should be marked to show the date the media was scanned and the bar code of the equipment used to perform the scanning.

3. If a virus appears at any other time, end users shall run antivirus software. If a virus is detected on a classified system, the end user must report it immediately to the antivirus administrator and the PSD to determine the source and impact of the virus.

4. End users shall request help from the IC if the antivirus software indicates a virus is still present or the infected file has been sent to quarantine.

5. The antivirus administrator shall review and attempt to clean up all infected files sent to quarantine. If the antivirus administrator cannot clean up the infected files, he or she shall consult with the manufacturer of the antivirus software or other sources for help.

6. End-users shall follow any instructions about virus attacks in electronic mail messages within one (1) hour of reading the electronic mail message.

7. End users shall report suspected virus attacks to the IC in accordance with reference c. The OIG Component Heads shall determine internal reporting procedures.

8. If a virus affects more than one microcomputer or if a virus affects a network server, the ISD shall prepare and oversee execution of a virus eradication plan.

9. End users at 400 Army Navy Drive and 1111 Jefferson Davis Highway or those connected by frame relay to the LAN/WAN shall update virus definitions if he or she has not logged on to the network for five (5) or more days. The following steps shall be used to perform the update:

- a. Select Start.

- b. Select Programs.
- c. Select Norton AntiVirus Corporate Edition.
- d. Select Live Update.

10. End users connecting to the LAN/WAN by a dial-up connection shall update virus definitions every five (5) days, as follows:

- a. Select Start.
- b. Select Programs.
- c. Select Norton AntiVirus Corporate Edition.
- d. Select Live Update.

11. If a person who works at 400 Army Navy Drive or 1111 Jefferson Davis Highway is on temporary duty (TDY) for more than five (5) days, he or she should connect to the Remote Access Server (RAS) and use the steps in paragraph H.9. to update the virus definition files.

I. Effective Date. This Instruction is effective immediately. The OIG components may supplement this Instruction.

FOR THE INSPECTOR GENERAL:

/signed/
Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

**APPENDIX A
REFERENCES**

- a. IGDR 1400.4, *Disciplinary and Adverse Action*, December 30, 1994
- b. IGDINST 7950.2, *Inspector General Microcomputer Hardware and Software Management Program*, May 23, 2000
- c. IGDINST 7920.51, *Resolving End User Problems*, May 23, 2000
- d. DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AIS),” March 21, 1988
- e. IGDINST 7920.5, *Inspector General Small Computer Use*, August 18, 2000
- f. IGINST 5200.40, *Security Requirements for Automated Information Systems*, July 20, 2000
- g. DoD 5200.28 M, “ADP Security Manual,” January 1973

APPENDIX B DEFINITIONS

1. **Bootable** means that a diskette, Zip disk, compact disk (CD), or other type of media holds a set of instructions that can start or restart a computer system by reading initialization instructions into the computer's memory.
2. **Bootleg Software** refers to the illegal duplication and distribution of software and software documentation. Bootleg takes two specific forms--counterfeit and pirate.
 - a. **Counterfeit software**--the unauthorized simulation of prewritten programs, as well as the unauthorized duplication of original artwork, labels, trademarks, and packaging of prewritten programs produced by obtaining a legitimate copy of the software and simulating the functions.
 - b. **Pirate software**--the unauthorized duplication of legitimate copies of programs produced by procuring legitimate copies of software and duplicating them without having a license to make the copies.
3. **Chief Information Officer (CIO)** is the senior official appointed by the Inspector General, DoD, who is responsible for developing and implementing information resources management in ways that enhance OIG, DoD, mission performance through the effective, economic acquisition and use of information. The CIO is currently the Director of OA&IM.
4. **End User** is an OIG, DoD, employee or contractor who uses computer hardware or software to perform work-related tasks.
5. **Environment** includes the mode of operation of an information system, the hardware, the software, the internal operating system, and any external operating systems. Those operating systems include, but are not limited to, DOS, Windows, UNIX, Intranet, and Internet.
6. **Hardware** is equipment supporting an automated information system. An information system is the organized collection, processing, transmission, and dissemination of information according to defined procedures.
7. **Information** is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, maintained in any medium, including but not limited to, computerized data bases, paper, microform, or magnetic tape.
8. **Microcomputers** are computers that have self-contained processing units and are easily transportable. The definition includes, but is not limited to, equipment that may be referred to as palmtop computers, hand held computers, personal digital assistant computers, personal computers, desktop computers, laptop computers, and notebook computers.
9. **Program** is a series of instructions that shall cause a computer to perform tasks.
10. **Software** is a program that tells a computer what to do.
11. **System** is a collection of people, equipment, policies, and methods organized to accomplish an activity.
12. **Virus**, as used in this Instruction, includes all malicious software, such as:

IGDINST 7950.4

- a. Bombs--programs with a trigger for perpetration of a malicious act when particular states of the system are realized.
- b. Trap doors--hidden commands or entry points into a program module that can be triggered to permit circumvention of system protection mechanisms.
- c. Trojan horses--programs with a documented legitimate function (actual or apparent) that additionally performs some hidden unauthorized action(s).
- d. Worms--programs that can replicate themselves without becoming an attachment to any other software.
- e. A true virus, defined as malicious code, has the ability to locate other software and make copies of other software and embed itself within the software.

13. **Write-Protect** means to place a write-protect tab on a 5 $\frac{1}{4}$ " diskette, or to open the slide on a 3 $\frac{1}{2}$ " diskette to expose the write-protect hole.